CLASS SPECIFICATION
County of Fairfax, Virginia

CLASS CODE: 1830 **TITLE:** INFORMATION SECURITY ANALYST I **GRADE:** S-24

DEFINITION:

Under general supervision, assists with the design, implementation, and monitoring of information protection activities in distributed and mainframe environments within the County for County-wide systems; typically works under the leadership and tutelage of a higher-level analyst; and performs related work as required.

DISTINGUISHING CHARACTERISTICS OF THE CLASS:

Positions assigned to this class perform entry level information protection analysis work. The work of this class is distinguished from the work of an Information Security Analyst II in that the Information Security Analyst II performs work such as independently evaluating security-related functions and implementing strategies for system and network software; recommending changes and enhancements to meet security requirements; and monitoring software modifications and security controls throughout the system. The Information Security Analyst I class would not perform duties such as these independently but would assist or participate in them under the leadership of a higher-level analyst.

ILLUSTRATIVE DUTIES:

Provides information protection related support functions such as selective administration of identification and authentication functions, access control functions for selected platforms and activities, and the provision of anti-virus software to County agencies;
Assists in the conduct of threat analysis for current and evolving automated information processing technologies;
Assists in identifying risks and vulnerabilities to current and planned automated information processing technologies;
Assists in identifying and evaluating the effectiveness of countermeasures designed to minimize or neutralize system vulnerabilities;
Prepares findings in written and oral formats;
Assists in preparing and documenting information protection plans, policies, and procedures;
Provides assistance to other staff as needed.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES:

Some knowledge of automated information processing capabilities, functions, and concepts;

Some knowledge of information protection concepts, capabilities, and functions;

Ability to identify potential systems threats, vulnerabilities, and risks;

Ability to identify countermeasures to manage system risks and vulnerabilities;

Ability to express thoughts in writing and orally to individuals at all levels of the organization;

Ability to follow written and verbal instructions;

Ability to analyze information and reach conclusions and formulate such thoughts into written and oral plans of actions;

Ability to work with sensitive information and maintain confidentiality of such data and information;

Ability to provide information protection advice and assistance to technical and non-technical individuals at all levels of the organization;

Ability to understand and explain technical terms and concepts in a non-technical manner.

EMPLOYMENT STANDARDS:

Any combination of education, experience, and training equivalent to the following:

Possession of a bachelor’s degree in a computer science field of study, electrical engineering, or telecommunication management; a business degree with computer science course work; or a bachelor’s degree in an associated field of study with course work in computer science.

CERTIFICATES AND LICENSES REQUIRED:

None.

ESTABLISHED: May 24, 1999